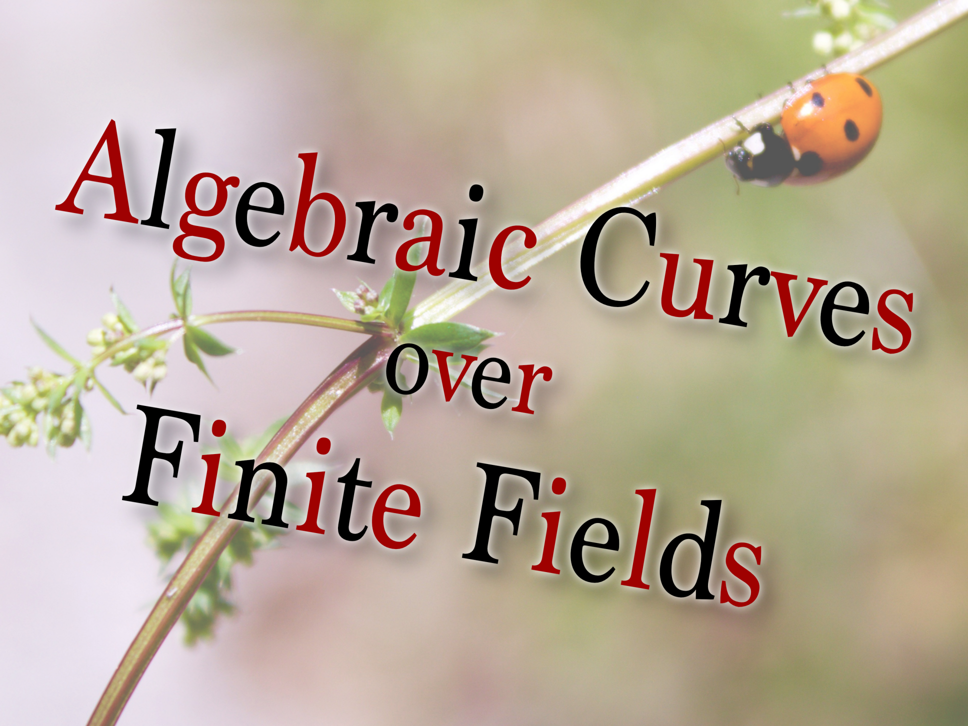

Algebraic Curves
over
Finite Fields

Who am I?

Where & when to find me

- ANNAMARIA IEZZI

  Post-doc in Mathematics at USF

- WHERE?

  Physically → Office CMC 110

  Online → www.aiezzi.it

  aiezzi@usf.edu

You can find here a webpage of this course!

- WHEN?

  Mondays
  Wednesdays } → 5-6 pm

Course Information

Time and location of classes

Mondays
Wednesdays } 3:30 – 4:45 pm in CMC 109

Note: On Monday 2–3pm there is normally the "Discrete Mathematics Seminar" in CMC 108

Prerequisites

A reasonable background in abstract algebra (group theory, ring theory, field theory, Galois theory, ...)

No textbook is required!

... but for each class all the references will be given.

EVALUATION

Will be based on:

- **2 HOMEWORK ASSIGNMENTS**
  Due approximately during week 6 and 11 of the semester
  50 % final grade

- **FINAL PROJECT (oral presentation)**
  50 % final grade

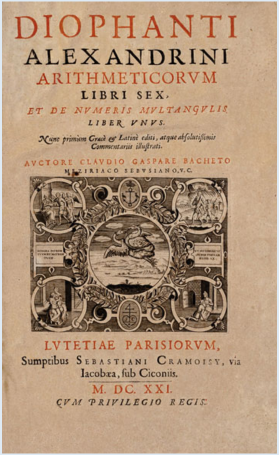
BACK
to the
PAST


3rd century AD
HADRIAN'S WALL
LONDON
ROME
BYZANTIUM
ATHENS
SYRACUSE
CARTHAGE
BABYLON
ALEXANDRIA
JERUSALEM
CYRENE
Intellectual and cultural center of the ancient world for some time
ROMAN EMPIRE
3rd century AD

DIOPHANTUS

of Alexandria

- Born probably at the beginning of the 3rd century AD.
- Called sometimes the "Father of Algebra".
- Credited as the first Greek (?) mathematician who recognized fractions as numbers.
- His most notable publication is "Arithmetica".



Cover of the 1621 edition translated into Latin from Greek by Claude Gaspard Bachet de Méziriac.

Arithmetica

- Series of 13 books written in Greek (only 6 survived)

- collection of 130 algebraic problems giving numerical solutions of indeterminate polynomial equations.

"Knowing, my most esteemed friend Dionysius, that you are anxious to learn how to investigate problems in numbers, I have tried, beginning from the foundations on which the science is built up, to set forth to you the nature and power subsisting in numbers".

*polynomial equations

BOOK I: indeterminate equations* of first degree

BOOKS II-III: indeterminate equations* of second degree

BOOKS IV-V: indeterminate equations* of third and fourth degree

solutions in $\mathbb{Q}^+$

Problem 8
Book II

: To divide a given square number in two squares.

Given square 16.

DIOPHANTUS'S SOLUTION

x^2 one of the required squares.

Thus $16 - x^2$ has to be a square

Take a square of the form:

$$(mx - 4)^2,$$

square root of 16

m being any integer.

E.g: take $(2x-4)^2$, and set it equal to $16-x^2$:

$$4x^2 - 16x + 16 = 16 - x^2 \Rightarrow 5x^2 = 16x \Rightarrow x = \frac{16}{5}.$$

A pair of required squares is then $\frac{256}{25}$ and $\frac{144}{25}$

Some remarks

- Most of the times Diophantus, by making appropriate choices, uses only one variable for the unknown to solve the problem.

- The object of Diophantus' problems is simply finding a solution to an indeterminate equation and not to list all the solutions.

- Diophantus does not accept non-positive numbers as solutions.

WARNING!

Nowadays with the name

"Diophantine equations"

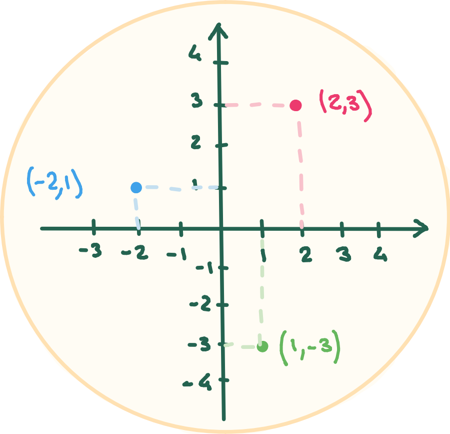
(named in honor of Diphantus) we refer to polynomial equations, usually in two or more unknowns such that only the integer solutions are sought or studied.

$\mathbb{Z}$

<u>Note</u>: rational solutions of $x^2+y^2=16$ corresponds to integer solutions of $X^2+Y^2=16Z^2$ and viceversa.

What do Diophantus' equations have to do with ALGEBRAIC CURVES

In the 17th century René Decartes introduces the Cartesian coordinate system...



Problem 8 Book II

: To divide a given square number in two squares.

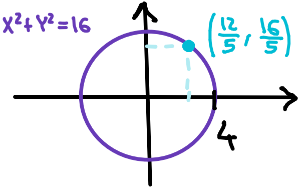
Given square 16.

GEOMETRICAL INTERPRETATION

Equivalent to find two positive rational numbers X and Y such that:

$$16 = X^2 + Y^2$$ → POLYNOMIAL EQUATION

i.e. find a point $(x, y) \in \mathbb{Q}^+ \times \mathbb{Q}^+$ on the plane algebraic curve $\mathcal{C} : X^2 + Y^2 = 16$.



→ such a point is called, in modern terms, a rational point! (since its coordinates are rational numbers)

In modern terms we can say that Diophantus studied in his ARITHMETICA the structure of $\mathbb{Q}^+$-rational points

* All curves considered by Diophantus were of genus 0 or 1.

* One of his methods corresponds geometrically in finding a rational parametrization of curves of genus 0.

Diophantus' work led to one of the greatest math challenges of all times...

Again during the 17th century, the problem II:8 of Arithmetica:

"To divide a given square number into two squares".

catched the attention of the French mathematician

Pierre de Fermat

who was trying to generalize some problems in Arithmetica.

A too small margin ...

teruallo quadratorum, & Canones iidem hic etiam locum habebunt, vt manifestum est.

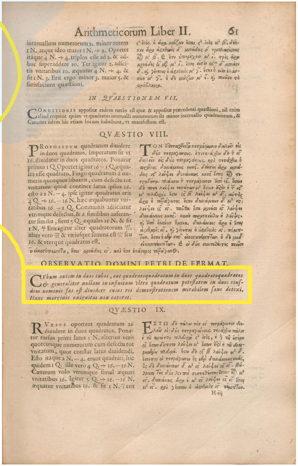
QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quot continet latus ipsius 16. esto à 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$. & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

ΤΟΝ ἐπιταχθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους. ἐπιτετάχθω δὴ τὸν ις διελεῖν εἰς δύο τετραγώνους. καὶ τετάχθω ὁ πρῶτος δυνάμεως μιᾶς. δεήσει ἄρα μονάδας ις λεῖψει δυνάμεως μιᾶς ἴσας εἶναι τετραγώνῳ. πλάσσω τὸ τετράγωνον ἀπὸ ςς. ὅσων δή ποτε λεῖψει τοσούτων μο. ὅσων ἐστὶν ἡ τοῦ ις μο. πλευρά. ἔστω ςς β λεῖψει μο. δ. αὐτὸς ἄρα ὁ τετράγωνος ἔσται δυνάμεων δ μο. ις [λεῖψει ςς ις.] ταῦτα ἴσα μονάσι ις λεῖψει δυνάμεως μιᾶς. κοινὴ προσκείσθω ἡ λεῖψις, καὶ ἀπὸ ὁμοίων ὅμοια. δυνάμεις ἄρα ε ἴσαι ἀριθμοῖς ις. καὶ γίνεται ὁ ἀριθμὸς ις πέμπτων. ἔσται ὁ μὲν σνς εἰκοστοπέμπτων. ὁ δὲ ρμδ εἰκοστοπέμπτων, καὶ οἱ δύο συντεθέντες ποιοῦσι υ εἰκοστόπεμπτα, ἤτοι μονάδας ις. καὶ ἔστιν ἑκάτερος τετράγωνος.

The most famous mathematical MARGINAL NOTE

"Cubem autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet."



Arithmeticorum Liber II. 61

interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superaddere 10. Ter igitur 2. adscitis vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & satisfaciunt quæstioni.

IN QVAESTIONEM VII.

CONDITIONIS appositæ eadem ratio est quæ & appositæ præcedenti quæstioni, nil enim aliud requirit quàm vt quadratus interualli numerorum sit minor interuallo quadratorum, & Canones iidem hic etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum a numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto a 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & a similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter vero $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. − 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. − 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. − 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{16}{5}$ erit

H iij

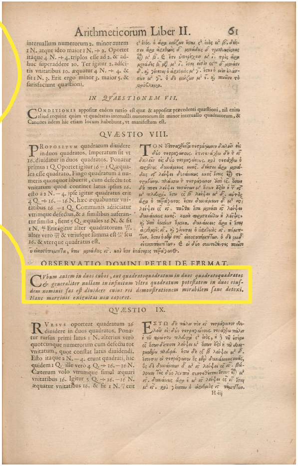
The 1670 edition of Diophantus' produced by Fermat's son includes Fermat's commentary particularly his "Last Theorem"

"On the other hand, it is impossible to separate a cube into two cubes, or biquadrate into two biquadrates, or generally any power exept a square into two powers with the same exponent. I have discovered a truly marvellous proof of this, which, however, the margin is not large enough to contain".

The most famous mathematical MARGINAL NOTE

"Cubem autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet."

"On the other hand, it is impossible to separate a cube into two cubes, or biquadrate into two biquadrates, or generally any power exept a square into two powers with the same exponent. I have discovered a truly marvellous proof of this, which, however, the margin is not large enough to contain".


Arithmeticorum Liber II. 61

interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superaddere 10. Ter igitur 2. adscitis vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & satisfaciunt quæstioni.

IN QVÆSTIONEM VII.

CONDITIONIS appositæ eadem ratio est quæ & appositæ præcedenti quæstioni, nil enim aliud requirit quàm vt quadratus interualli numerorum sit minor interuallo quadratorum, & Canones iidem hic etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum a numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto a 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & a similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter vero $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. − 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. − 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. − 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{16}{5}$ erit

The 1670 edition of Diophantus' produced by Fermat's son includes Fermat's commentary particularly his "Last Theorem"

Fermat's Last Theorem

The Diophantine equation

$$X^n + Y^n = Z^n$$

has no non-trivial integer solution for $n > 2$.

The polynomial equation

$$X^n + Y^n = Z^n$$

corresponds in the complex projective plane $\mathbb{P}^2(\mathbb{C})$ to a projective algebraic plane curve, called

THE FERMAT CURVE.

→ Affine equation: $x^n + y^n = 1$.

Fermat's Last Theorem states that the Fermat curve has no points $(X:Y:Z)$ with integer coordinates for $n > 2$.

(and equivalently the affine curve has no $\mathbb{Q}$-rational points when $n > 2$).

Finite Fields

are coming...

The Diophantine equation

$$x^n + y^n + z^n = 0$$

can be reduced modulo a prime number p:

$$(\star) \quad x^n + y^n + z^n \equiv 0 \mod p,$$

and we can consider solutions to this equation in the FINITE FIELD

$$\frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p = \{0, 1, \ldots, p-1\}.$$

In particular, the equation $(\star)$ has a finite number of solutions in $\mathbb{F}_p$.

$$\#\text{solutions} \leq |\mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p| = p^3.$$

Analogously, we can look for points $(x:y:z)$ with coordinates in $\frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p = \{0, 1, \ldots, p-1\}$ on the Fermat curve defined over $\mathbb{F}_p$:

$$C_n : x^n + y^n + z^n \equiv 0 \mod p.$$

e.g.: If $p=3$, then $(1:1:1)$ is a point on the Fermat curve defined over $\mathbb{F}_3$. We call it a $\mathbb{F}_3$-rational point.

Now the curve has a finite number of $\mathbb{F}_p$-rational points:

$$\underbrace{\#\,\mathbb{F}_p\text{-rational points}}_{\#\,C_n(\mathbb{F}_p)} \leq \#\,\mathbb{P}^2(\mathbb{F}_p) = \frac{p^3-1}{p-1} = p^2+p+1$$

Can we count the number of rational points on an algebraic curve defined over a finite field

CARL FRIEDRICH GAUSS was probably the first one to count the number of rational points on several types of curves defined over the prime field $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$.

DISQUISITIONES ARETHMETICAE

§ 358

$$C_3 : x^3 + y^3 + z^3 \equiv 0 \pmod p$$

with $p > 3$.

- if $p \not\equiv 1 \pmod 3$ then

  $$\# C_3(\mathbb{F}_p) = p+1$$

- if $p \equiv 1 \pmod 3$ there is a unique way of writing $4p = a^2 + 27b^2$ with $a, b \in \mathbb{Z}$ and $a \equiv 1 \pmod 3$, and

  $$\# C_3(\mathbb{F}_p) = p+1+a$$

Note: $|a| < 2\sqrt{p}$

Gauss calculated:

- $\# C_2(\mathbb{F}_p)$ (when $n=2$)
- $\# C_3(\mathbb{F}_p)$ (when $n=3$)

When $n>3$ things get progressively more complicated and in general there is only one estimate:

$$\left| \# C_n(\mathbb{F}_p) - (p+1) \right| \leq \left[2g\sqrt{p} \right]$$

where $g = \dfrac{(n-1)(n-2)}{2}$.

SPOILER ALERT

This is a particular case of a deep result in Algebraic Curve Theory, namely the so-called HASSE-WEIL BOUND...

What do I do with algebraic curves defined over finite fields

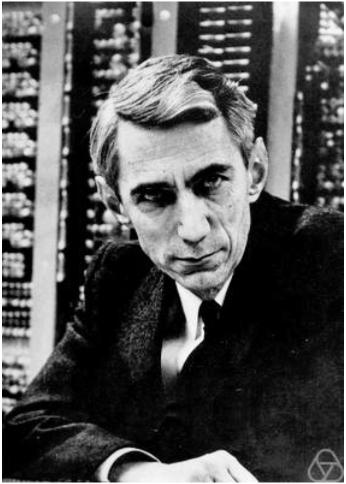
CLAUDE SHANNON
(1916 - 2001)

- Mathematician, electrical engineer and cryptographer

- The father of
  INFORMATION THEORY

  1948: "A mathematical theory of communication"
  How best to encode the information a sender wants to transmit

- First to use the word "bit" (= portmanteau of binary digits).



TWO BRANCHES OF INFORMATION THEORY

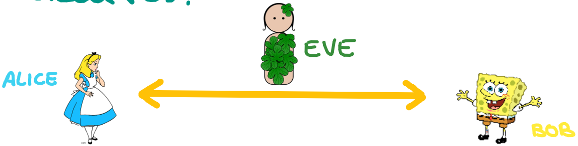
→ CODING THEORY

study of the properties of CODES, used for data compression, transmission and storage

- Error-correcting codes
  codes that allow to control errors in data transmission over noisy channels: REDUNDANCY

→ CRYPTOGRAPHY

study of techniques for secure communication in the presence of third parties called adversaries.



ALGEBRAIC CURVES OVER FINITE FIELDS IN INFORMATION THEORY

→ CODING THEORY

Algebraic geometric code (AG-code, Goppa code): linear code constructed using an algebraic smooth curve defined over $\mathbb{F}_q$ (with many $\mathbb{F}_q$-rational points.

→ CRYPTOGRAPHY

ELLIPTIC CURVES

- Elliptic-curve cryptography (ECC)
  ~ 1985
- isogeny-based cryptography
  ~ 1995

OUTLINE OF THE COURSE

- Algebraic geometric approach
  - * over algebraically closed fields
  - * over perfect fields
    - review some facts of field theory (finite fields)
- Algebraic function fields of one variable
  (algebraic approach)
- The zeta function and the Riemann Hypothesis for curves over finite fields
- Applications
  - * coding theory
  - * cryptography

PRINCIPAL REFERENCES

1) Fulton: "Algebraic curves: an introduction to Algebraic Geometry".

2) Silverman: "The Arithmetic of Elliptic Curves."
E-book at USF Library

3) Stichtenoth: "Algebraic function fields and Codes"
E-book at USF Library

4) Tsfasman, Vlăduţ, Nogin: "Algebraic Geometric Codes: Basic Notions"

E-book at USF Library

5) Several articles

WELCOME TO THE

OF ALGEBRAIC CURVES

OVER

FINITE FIELDS

NEXT TIME:

Plane Curves